METHOD FOR IDENTIFICATION BASED ON BILINEAR DIFFIE-HELLMAN PROBLEM

FIELD OF THE INVENTION

The present invention relates to an identification scheme; and, more particularly, to a method for user identification in network environments, based on the bilinear Diffie-Hellman problem.

BACKGROUND OF THE INVENTION

Currently, diverse off-line services are expanding their ranges to cyberspace through internet as a result of steady development of network environments. In cyberspace, remote non-face-to-face interconnections can be made anytime and anywhere. However, such non-face-to-face circumstances bring about an identification (ID) problem of distinguishing legitimate users from illegitimate ones. In general, an identification scheme means a cryptographic technique employed to solve an identification problem in non-face-to-face circumstances such as cyberspace interactions.

A most basic identification scheme uses identification (ID) information particular to each user and password information only one user knows. Most UNIX operating systems employ this type of scheme. However, this scheme leaves room for masquerade attacks because a user's password can be easily exposed during its transmission through a communication channel.

In order to overcome the drawback described above, identification schemes employing public-key cryptographic system have been developed. This scheme is applied to such fields as, for example, cyberbanking. In a public-key cryptographic system, a public key and a private key are used. Typcally, the private key is known to nobody except its owner, and the public key is available to public. A prover, who is expected to know the private key, requests a service to a verifier. The prover tries to prove himself a legitimate user by showing that he knows the private key corresponding to the public key, while not divulging the private key. And the verifier tries to verify the prover's legitimacy only by utilizing information disclosed by the prover.

Identification schemes employing the public-key cryptographic system based on number theory can be classified into two categories, i.e., one based on the factorization problem, e.g., the Fiat-Shamir scheme, and the other, e.g., the Schnorr scheme, based on the discrete logarithm problem.

The procedure of the Fiat-Shamir scheme can be expounded as follows. A reliable system administrator selects a sufficiently large number n. Then, A prover selects his own private key a that is relatively prime with n, and calculates $b = a^2$ mod n. The prover discloses b. Then, the following protocol is repeated for a number of times:

(a) The prover selects a random integer r □ Z_n^*, where Z_n^* is a multiplicative group of order n, calculates $x = r^2$, and sends x to the verifier;

(b) The verifier selects a random number □ □ {0, 1}, and sends □ to the prover;

(c) On receiving □, the prover calculates $y = r$□ $a^{□}$ mod n and sends y to the verifier; and

(d) The verifier examines whether $y^2 = x$□$b^{□}$ mod n is established. If true, then the verifier accepts the prover as a legitimate user and, otherwise, stops the protocol.

Various schemes have been developed based on the original Fiat-Schamir scheme, and follows the above-mentioned protocol.

On the other hand, the procedure of the Schnorr scheme is as follows. First, two primes numbers p and q are chosen, wherein q is a prime factor of p-1. Then, choose a not equal to 1, such that a^q □ 1 (mod p). Then, a random number s, i.e., the private key, less than q is chosen. The public key $v = a^{-s}$ mod p is then calculated. Thereafter, the following protocol is executed:

(a) The prover selects a random number r less than q, and computes $x = a^r$ mod p, then sends x to the verifier;

(b) The verifier sends the prover a random number □ □ Z_q^*, where Z_q^* is a multiplicative group of order q;

(c) The prover computes $y = r + s$□ mod q and sends y to the verifier; and

(d) The verifier verifies whether $x = a^y$ □$v^{□}$ mod p is established. If true, then the verifier accepts the prover as a legitimate user and, otherwise, stops the protocol.

However, the aforementioned schemes have the following drawbacks. As for the Fiat-Shamir scheme, three demerits may be pointed out. First, its security proof is too intricate to demonstrate. The security of the Fiat-Shamir scheme has been proved by employing an interactive zero-knowledge proof based on complexity theory, which is too complicated to be grasped intuitively. Most state-of-the-art schemes based on the Fiat-Shamir scheme also employ the zero-knowledge proof to show their security. Second, a query-and-response procedure needs to be reiterated a number of times between the prover and the verifier, thereby causing computational overheads. Third, this scheme is based on prime factorization problem, which needs longer keys than those of discrete-logarithm-problem-based schemes.

On the other hand, the Schnorr scheme has also two major shortcomings. First, this scheme requires a certificate, which has difficulties in its verification and revocation. Second, this scheme is practical only when an identification is performed among systems which have greatly different computing powers, e.g., a server and a client, but not between a server and another server.

SUMMARY OF THE INVENTION

It is, therefore, an object of the present invention to provide an identification scheme based on discrete logarithm problem, requiring no certificate and including only one query-and-response procedure, of which security can be proved in an easily apprehensible way.

In accordance with a preferred embodiment of the present invention, there is provided a method for identification, including the steps of: (a) generating system parameters G_1, G_2, P and $\hat{e}$ and storing the system parameters in a memory by a system administrator, wherein G_1 and G_2 are cyclic groups of order m, P is a generator on the cyclic group G_1, $\hat{e}$ is a bilinear map defined as $\hat{e}: G_1 \times G_1 \mapsto G_2$; (b) generating a private key <a, b, c> and a public key v and storing the public key v in the memory by a prover or the system administrator, wherein a, b and c are randomly chosen in Z_m^* where Z_m^* is a multiplicative group of order m; (c) generating random numbers r_1, r_2, $r_3 \in Z_m^*$ for obtaining an evidence (x, Q) and sending the evidence (x, Q) to a verifier by the prover; (d) receiving the evidence (x, Q), selecting a randomly selected number ω □ Z_m^* to obtain a query R, storing the evidence (x, Q) and the randomly selected number ω in the memory and sending the query R to the prover by the verifier; (e) receiving the query R, computing a temporary value S to obtain a response Y and sending the response Y to the verifier by the prover; (f) determining a legitimacy of the prover by employing the system parameters G_1, G_2, P and $\hat{e}$, the public key v, the evidence (x, Q) and the randomly selected number ω by the verifier.

In accordance with another preferred embodiment of the present invention, there is provided a method for identification, including the steps of: (a) generating system parameters G_1, G_2, P and $\hat{e}$ and storing the system parameters in a memory by a system administrator, wherein G_1 and G_2 are cyclic groups of order m, P is a generator on the cyclic group G_1, $\hat{e}$ is a bilinear map defined as $\hat{e}: G_1 \times G_1 \mapsto G_2$; (b) generating a private key $<a_1, a_2, \ldots a_n>$ and a public key v and storing the public key v in the memory by a prover or the system administrator, wherein a_1, a_2, ... a_n are randomly chosen in Z_m^* where Z_m^* is a multiplicative group of order m; (c) generating random numbers $r_1, r_2, \ldots r_n \in Z_m^*$ for obtaining an evidence (x, Q) and sending the evidence (x, Q) to a verifier by the prover; (d) receiving the evidence (x, Q), selecting a randomly selected number ω □ Z_m^* to obtain a query R, storing the evidence (x, Q) and the randomly selected number ω in the memory and sending the query R to the prover by the verifier; (e) receiving the query R, computing a temporary value S to obtain a response Y and sending the response Y to the verifier by the prover; (f) determining a legitimacy of the prover by employing the system parameters G_1, G_2, P and $\hat{e}$, the public key v, the evidence (x, Q) and the randomly selected number ω by the verifier.

BRIEF DESCRIPTION OF THE DRAWINGS

The above and other objects and features of the present invention will become apparent from the following description of preferred embodiments given in conjunction with the accompanying drawings, in which:

Fig. 1 represents a conceptual diagram of interactions among participants of an identification scheme in accordance with the present invention;

Fig. 2 depicts a flow chart showing a protocol of an identification scheme in accordance with the present invention; and

Fig. 3 illustrates a flow chart showing a method for identification based on bilinear Diffie-Hellman problem in accordance with a preferred embodiment of the present invention.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

Referring to Fig. 1, there is illustrated a conceptual diagram of interactions among participants of an identification scheme in accordance with the present invention. The participants, which may be implemented by using computer systems, are a prover, a verifier and a system administrator.

Each of the participants plays its role as follows. The system administrator, only active during system initialization, generates and discloses system parameters. In some cases, the system administrator may also generate a pair of public and private keys for the prover using the system parameters to thereby send the generated keys via a secure channel. In other cases, the prover may generate the pair of public and private keys. The prover tries to prove itself a legitimate user by submitting some information to the verifier. The verifier verifies a validity of the submitted information with reference to the system parameters, and then determines whether the prover is a legitimate user by means of the submitted information and the public key.

Referring to Fig. 2, the identification scheme in accordance with the present invention includes the steps for generating system parameters and a pair of public and private keys (step 100); requesting a service and submitting an evidence to the verifier by the prover (step 110); performing query and response by the prover and the verifier (step 120); performing ID verification by the verifier (step 130); the determining the prover's legitimacy by the verifier (step 140); and performing service denial or access allowance by the verifier (step 150 or 160).

In the step for generating system parameters and the pair of public and private keys (step 110), the system administrator discloses the system parameters to be shared by both the prover and the verifier. More particularly, cyclic groups G_1 and G_2 of order m, and a generator P on the cyclic group G_1 are randomly selected. And next, a bilinear map is defined in relation to the two cyclic groups. Besides, the prover or the system administrator generates the public and the private keys of the prover.

In the step for service request and evidence submission (step 120), the prover generates random numbers to thereby submit the evidence by using the system parameters disclosed by the system administrator.

Subsequently, the step for query and response (step 130), which includes the step for making the verifier send the query to the prover and the step for letting the prover compute the response by use of the private key and the query to thereby send the response to the verifier, is performed.

Thereafter, the steps for ID verification (step 130) and legitimacy determination (step 140) are performed sequentially, and then the step for service denial (step 150) or allowance (step 160) follows. The verifier examines the query and the public key corresponding to the prover's private key (step 130) and determines the prover's legitimacy (step 140). Then, a service access is denied if the prover is determined to be illegitimate (step 150) and allowed otherwise (step 160).

Hereinafter, a method for identification based on bilinear Diffie-Hellman problem in accordance with a preferred embodiment of the present invention will be explained in more detail with reference to Fig. 3.

First, the system administrator generates system parameters, such as G_1, a group of points on an elliptic curve, and G_2, a finite field, each of G_1 and G_2 having an order m (step 200). Next, a generator P on the cyclic group G_1 is selected randomly. And then, a transformed bilinear map is defined. This map is expressed as the following equation.

$$\hat{e}: G_1 \times G_1 \mapsto G_2 \qquad Eq.(1)$$

All the system parameters, G_1, G_2, P and $\hat{e}$, are stored in a memory.

Next, the prover or the system administrator generates a public key and a private key by using the system parameters (step 210). Random values a, b, and c belonging to Z_m*, where Z_m* is a multiplicative group of order m, are chosen as the private key. Employing the following equation, the public key v is obtained.

$$v=\hat{e}(P,P)^{abc}$$

Eq.(2)

The prover or the system administrator publishes the public key v, while the private key being kept secret. The published public key can be obtained by the verifier whenever needed. The public key is stored in the memory.

Subsequently, the prover selects random numbers r_1, r_2, r_3 □ Z_m^* and generates an evidence for identifying the prover by computing the following equation (step 220).

$$x=\hat{e}(P,P)^{r_1r_2r_3},\ Q=r_1r_2r_3P$$

Eq.(3)

The prover sends the evidence (x, Q) to the verifier. The evidence includes two evidence values, i.e., a first evidence value $x=\hat{e}(P,P)^{r_1r_2r_3}$ and a second evidence value $Q=r_1\,r_2\,r_3\,P$, so that the random numbers r_1, r_2 and r_3 can be effectively protected from forgery or alteration.

The verifier receives the evidence (x, Q), selects a randomly selected number ω □ Z_m^* and computing a query R to thereby send it to the prover (step 230). The evidence (x, Q) and the randomly selected number ω are stored in the memory. For keeping the query safe from being forged or changed during transmission, the randomly selected number ω is transformed into a value R belonging to the cyclic group G_1 to be sent as the query. The query R can be obtained by using the following equation.

$$R=\omega P \qquad \textit{Eq.(4)}$$

Next, the prover receives the query R and then calculates a temporary value S by employing the following equation (step 240).

$$S=r_1r_2r_3R \qquad \textit{Eq.(5)}$$

Thereafter, the prover computes a response Y to submit it to the verifier, wherein the temporary value S is used for protecting the response Y from forgery or change during a transmission. The computation of the response Y is performed as the following equation.

$$Y=abcP+(a+b+c)S \qquad \textit{Eq.(6)}$$

As shown in Eq. (6), only three arithmetic operations, i.e., two scalar multiplications (for the terms *abcP* and (*a*+*b*+*c*)*S*) and one addition (for the term *abcP*+(*a*+*b*+*c*)*S*), are sufficient for generating the response *Y*, so that a computational overhead can be reduced in accordance with the present invention.

The verifier receives the response *Y* and then checks a validity of the prover by using the following equation (step 250).

$$x=\hat{e}(P,Q) \qquad \textit{Eq.(7)}$$

If Eq.(7) is not established, the prover is an invalid user; otherwise, the following equation is computed.

$$\hat{e}(Y,P)=v\ \hat{e}(aP+bP+cP,\ Q)^{\omega}$$

Eq.(8)

If Eq.(8) is true, the prover is a legitimate user; if not, an illegitimate user.

Finally, the verifier sends the prover the above verification result, i.e., a service denial for an invalid or illegitimate user and an access allowance for a legitimate user (step 260).

As described above, the identification scheme of the present invention enables the prover to prove himself a legitimate user after only three times of interactions without disclosing his private information.

Although the number of elements of the private key is three and the number of the random numbers is three in the preferred embodiment of the present invention, the number of elements of the private key and the number of the random numbers can be changed to other numbers.

While the invention has been shown and described with respect to the preferred embodiments, it will be understood by those skilled in the art that various changes and modifications may be made without departing from the spirit and the scope of the invention as defined in the following claims.